ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 31505—2015

# 信息安全技术　主机型防火墙安全技术要求和测试评价方法

**Information security technology—Technique requirements and testing and evaluation approaches for host-based firewall and personal firewall**

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部计算机信息系统安全产品质量监督检验中心、中国电子技术标准化研究院、北京启明星辰技术股份有限公司、公安部第三研究所。

本标准主要起草人:陆臻、顾健、韦湘、俞优、邓琦、罗锋盈、许玉娜、张笑笑、吴其聪。

# 信息安全技术　主机型防火墙<br>安全技术要求和测试评价方法

## 1　范围

本标准规定了主机型防火墙的安全技术要求、测评评价方法及安全等级划分。

本标准适用于主机型防火墙的设计、开发与测试。

## 2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2008　信息技术　安全技术　信息技术安全性评估准则　第3部分：安全保证要求

GB/T 25069　信息安全技术　术语

## 3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

**主机型防火墙　host-based firewall and personal firewall**

又称基于主机的防火墙或个人防火墙，是一个运行于单机上的软件。它可以监测主机上进行的入站和出站网络连接，并能够通过预先定义的规则，执行基于网络地址和基于应用的访问控制，通常还具有反恶意软件，入侵检测和网络告警等其他安全功能。

3.2

**安全策略　security policy**

指有关管理、保护安全域节点的规定和策略。

## 4　主机型防火墙描述

主机型防火墙以软件形式安装在最终用户计算机(包括个人计算机和服务器)上，阻止由外到内和由内到外的威胁。主机型防火墙不仅可以监测和控制网络级数据流，而且可以监测和控制应用程序，弥补网关防火墙和防病毒软件等传统防御手段的不足。此外，一般运行于服务器上的主机型防火墙还可以对所有的节点进行统一控制，实施统一的安全策略与响应。

主机型防火墙保护的资产是受安全策略保护的主机服务和文件等。此外，主机型防火墙软件本身及安全策略等重要数据也是受保护的资产。